Audyt za 1 zł

Bardzo szybko wzrasta liczba ataków i incydentów w obszarze cyberbezpieczeństwa. Dotykają one również podmiotów publicznych, w tym także małych jednostek samorządu terytorialnego (JST). Obowiązek wykonania audytu określającego poziom bezpieczeństwa w JST wydaje się więc zasadny. Praktyka pokazuje jednak, że różne względy formalne i prawne często pozbawiają audyty wiarygodności.

Katarzyna Żółkiewska-Malicka

dyrektor ds. bezpieczeństwa informacji w ZETO sp. z o.o. w Lublinie. Audytor wewnętrzny, specjalista ds. bezpieczeństwa informacji z 20-letnim stażem pracy, w zakresie przeprowadzania audytów cyberbezpieczeństwa, bezpieczeństwa informacji, ochrony danych osobowych oraz audytów śledczych. Auditor Wiodący systemu zarządzania bezpieczeństwem informacji wg ISO/IEC 27001. Członek Stowarzyszenia Praktyków Ochrony Danych Osobowych oraz Stowarzyszenia Inspektorów Ochrony Danych SABI. Ekspertka w Cyber Women Community. Lider ISSA Polska Lublin, Stowarzyszenia do spraw Bezpieczeństwa Systemów Informacyjnych. Członek CSO Council Społeczności Dyrektorów Bezpieczeństwa Informacji.

Centrum Projektów Cyfrowa Polska w latach 2021–2022 ogłosiło projekty Cyfrowa Gmina, Cyfrowy Powiat. Jak można przeczytać na stronie www.gov.pl/web/cppc/cyfrowa-gmina: *pandemia COVID-19 pokazała, że w dzisiejszym świecie niezwykle ważne jest sprawne wykorzystywanie technologii cyfrowych przez samorządy. Załatwianie spraw w urzędach i nauka zostały przeniesione do sieci, w ramach trybu zdalnego. Niektóre z urzędów napotkały problemy w postaci np. braków sprzętowych czy niewystarczających kompetencji cyfrowych pracowników, a naukę zdalną utrudnił brak komputerów i problem z dostępem do Internetu, zwłaszcza wśród uczniów mieszkających na terenach popegeerowskich. W odpowiedzi na te problemy powstał projekt „Cyfrowa Gmina", w ramach którego: wesprzemy rozwój cyfrowy instytucji samorządowych, zwiększymy cyberbezpieczeństwo i zapewnimy sprzęt z dostępem do Internetu, niezbędny do nauki zdalnej.*

> *Cel programu to zwiększenie zdolności jednostek samorządu terytorialnego (JST) oraz podmiotów im podległych w zakresie realizacji e-usług, cyberbezpieczeństwa, pracy i nauki zdalnej.*

Zgodnie z par. 4 ust. 8 regulaminu grantowego Cyfrowa Gmina (tożsamy zapis dotyczył także Cyfrowego Powiatu) w ramach przyznanego Grantu obligatoryjna była realizacja zadania związanego z przeprowadzeniem diagnozy cyberbezpieczeństwa, zgodnie z zakresem oraz formularzem stanowiącym załącznik nr 8 do Regulaminu. Diagnoza cyberbezpieczeństwa musiała zostać przeprowadzona w terminie do 6 miesięcy od dnia zawarcia Umowy o powierzenie Grantu. W uzasadnionych przypadkach, po przekazaniu pisemnych wyjaśnień, Grantobiorca mógł przekazać diagnozę w terminie późniejszym, ustalonym z Beneficjentem. Po przeprowadzeniu diagnozy, Grantobiorca zobligowany był do przekazania wypełnionego formularza diagnozy (przeprowadzonej przez osobę posiadającą uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu) za pomocą elektronicznej skrzynki podawczej ePUAP do NASK na adres skrzynki: /NASK-Instytut/SkrytkaESP (akronim/temat: cyfrowa.gmina.diagnoza.cyber).

Każda z gmin oraz każdy powiat miał z góry określony budżet do wykorzystania. Jednostki objęte projektami otrzymały dofinansowanie w formie grantu do 100 proc. wydatków kwalifikowanych. Minimalna wartość grantu dla jednej gminy wynosiła 100 tys. zł, maksymalna – 2 mln zł. Dla jednego powiatu odpowiednio – od 100 tys. zł do 350 tys. zł. Wysokości grantu wskazują, że nacisk został położony na wsparcie małych gmin, które mają największe problemy z podnoszeniem poziomu cybrebezpieczeństwa z uwagi na niewielkie budżety. Wartość grantu była obliczana na podstawie liczby ludności w gminie oraz wskaźnika podstawowych dochodów podatkowych na 1 mieszkańca gminy przyjętego do obliczania subwencji wyrównawczej na 2021 r. publikowanego przez Ministerstwo Finansów.

Audyt w trakcie projektu

Ten zapis regulaminu spowodował problemy w dwóch obszarach związanych z przeprowadzaniem diagnozy cyberbezpieczeństwa.

Okres realizacji projektu grantowego wynosił maksymalnie 18 miesięcy, jednak nie później niż do 30.09.2023 r. Diagnoza cyberbezpieczeństwa musiała zostać przeprowadzona najpóźniej do 6 miesięcy od daty podpisania umowy. W większości przypadków gminy czekały z przeprowadzeniem audytu do granicznego terminu. Bez względu jednak na to, kiedy audyt został przeprowadzony, audytorzy w momencie jego przeprowadzania mieli świadomość, że raport szybko straci swoją aktualność. Dlaczego?

Realizacja projektu przedłużała się m.in. z powodu procedur przetargowych czy problemów z dostępnością sprzętu. Zdarzały się urzędy, w których diagnoza była przeprowadzana przed rozstrzygnięciem najważniejszych przetargów np. na wyposażenie serwerowni. Audytor mógł uwzględnić w raporcie jedynie sprzęt, oprogramowanie, które zostały zakupione, zamontowane lub wdrożone.

> *Nikt tak naprawdę nie wiedział, po co diagnozy są robione i w jaki sposób ich wyniki będą oceniane przez NASK. Włodarze gmin i powiatów mieli obawy, że w przypadku niskiej oceny w arkuszu diagnozy ich gmina będzie narażona na potencjalne kontrole organów państwowych.*

Z takimi obiekcjami spotykałam się wielokrotnie, audytowani próbowali wpłynąć na audytora i wyniki oceny poszczególnych obszarów. Nie do końca wiadomo, co diagnozy – przeprowadzane podczas trwania realizacji projektu – oceniają. Nie były to ani diagnozy wstępne, oceniające poziom cyberbezpieczeństwa JST przed przystąpieniem do projektu (tzw. Stan „0"), ani też diagnozy końcowe, które

określiłyby faktyczny poziom bezpieczeństwa informacji po wydatkowaniu przyznanego grantu. Bardzo często audytor musiał decydować, czy uwzględnić w raporcie zakupiony sprzęt, ale jeszcze niedostarczony i niefunkcjonujący w jednostce. Narzucony termin przeprowadzenia diagnozy spowodował, że analizy przeprowadzone przez NASK są nieaktualne i nie odpowiadają rzeczywistości.

Przeszkody formalne

Drugim problemem okazał się sam załącznik nr 8, który stanowił wzór raportu z przeprowadzonej diagnozy. W pierwszej wersji dokument składał się z trzech arkuszy odnoszących się do: KRI (rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (KRI)), KSC (ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa) oraz COBIT, dotyczących oceny działalności wybranych procesów bezpieczeństwa.

W listopadzie 2021 r. arkusz został zaktualizowany poprzez usunięcie arkusza dotyczącego oceny działalności wybranych procesów bezpieczeństwa. W ostatecznej wersji załącznika JST te procesy były oceniane pod kątem spełnienia wymagań wynikających z KRI oraz stosowania i wywiązywania się z obowiązków wynikających z UoKSC. Kryteria oceny poszczególnych obszarów nie zostały określone, co sprawiło, że podczas przeprowadzania audytów te same obszary były odmiennie oceniane przez różnych audytorów.

Nie wiadomo było także, jak oceniać funkcjonowanie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) w jednostce. Czy samo opracowanie i wdrożenie Polityki ochrony danych osobowych oraz Instrukcji zarządzania systemem informatycznym jest tożsame z wdrożeniem SZBI? Nie ma żadnego przepisu jednoznacznie wskazującego, co na ten system się składa. Po zapoznaniu się z wynikami diagnoz przeprowadzanych przez innych audytorów mogę jednoznacznie stwierdzić, że obszar dotyczący SZBI był bardzo różnie interpretowany i oceniany przez audytorów. Zasadne wydaje się więc opracowanie jednoznacznych wytycznych i kryteriów, określających, co w poszczególnych obszarach poddajemy sprawdzeniu. Oczywiście, zaraz pojawią się głosy, że jeśli ktoś jest audytorem i posiada uprawnienia wynikające z rozporządzenia Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu, to powinien wiedzieć, jak poprawnie dokonać oceny. W praktyce wygląda to zupełnie inaczej. Certyfikaty wskazane w w/w rozporządzeniu dotyczą bardzo szerokiego zakresu tematyki bezpieczeństwa informacji. Wskazano tam certyfikaty dla osób sensu stricte związanych z IT, lecz także audytora wiodącego normy ISO 27001, który jest w stanie uzyskać osoba niebędąca informatykiem. Tak szeroki wachlarz osób uprawnionych do przeprowadzania audytu spowodował, że mieliśmy tak różne interpretacje zagadnień wskazanych w diagnozach. Miało to wpływ na wyniki, a tym samym na materiał poddawany analizie przez NASK.

PZP się kłania

Cyfrowa Gmina oraz Cyfrowy Powiat dotyczyły jednostek publicznych, które zobowiązane są stosować prawo zamówień publicznych (PZP). W zapytaniach ofertowych, ogłoszeniach w bazie konkurencyjności czy w przetargach wskazywane było jedyne kryterium – CENA. Wskazywano oczywiście wymóg posiadania przez audytora wymaganego certyfikatu, ale był to jedynie wymóg konieczny do złożenia oferty. Wygrywała po prostu najniższa cena. W nielicznych przypadkach należało wykazać się doświadczeniem w zakresie przeprowadzania audytów z zakresu bezpieczeństwa informacji. Im więcej firma była w stanie przedstawić referencji, tym większą liczbę punktów uzyskiwała. Niewielu klientom zależało, aby diagnoza była przeprowadzona przez podmiot profesjonalnie zajmujący się taką działalnością. Przeważająca większość potrzebowała po prostu wypełnionego załącznika podpisanego przez audytora posiadającego uprawnienia. Z przeprowadzonych kilkudziesięciu diagnoz na palcach jednej ręki mogę policzyć urzędy, które miały pytania do przesłanego raportu czy interesowały się ocenami poszczególnych obszarów. Diagnoza była traktowana jako element niezbędny do rozliczenia grantu i nic poza tym.

Audyt mógł przeprowadzić każdy posiadający uprawnienia wskazane w rozporządzeniu, mogły być to również osoby bez doświadczenia. Ponieważ wyniki przetargów lub zapytań ofertowych były publikowane na BIP, mieliśmy możliwość zapoznania się ze stawkami obowiązującymi na rynku. Ile może kosztować audyt wykonany przez profesjonalistę, który musiał zdobyć certyfikat potwierdzający jego umiejętności? Najtańsza oferta to 738 zł brutto i dotyczyła ona przeprowadzenia audytu cyberbezpieczeństwa w ramach Cyfrowego Powiatu. Spotykałam się już ze skrajnie niskimi cenami audytów bezpieczeństwa informacji czy cyberbezpieczeństwa, ale tym razem sięgnęliśmy bruku. Zdarzało się też często, że zapytania ofertowe czy OPZ zawierały dodatkowe czynności m.in. przeprowadzenie testów penetracyjnych. Niestety, również w takich przypadkach ceny można określić jako dumpingowe.

Oto zakres audytu cyberbezpieczeństwa w jednym ze Starostw Powiatowych:

1. Przeprowadzenie diagnozy cyberbezpieczeństwa.
2. Przeprowadzenie testów penetracyjnych obejmujących:
   - **a)** Skanowanie sieci – rekonesans sieci;
   - **b)** Skanowanie najistotniejszych hostów w sieci (serwery, kluczowe stacje końcowe, kamery, rejestratory), które zostały wybrane na podstawie wcześniejszej analizy;

c) Sprawdzenie domyślnych haseł dla najistotniejszych hostów w sieci (serwery, bramy, switche, access point), które zostały wybrane na podstawie wcześniejszej analizy.

3. Badanie ankietowe.

4. Testy socjotechniczne – końcowy termin wykonania zamówienia to 31.12.2023 r.

W trakcie wykonywania samej diagnozy cyberbezpieczeństwa weryfikujemy m.in.: dokumentację SZBI (cokolwiek klient pod tym kątem rozumie lub cokolwiek ma); zabezpieczenia fizyczne i środowiskowe; urządzenia brzegowe; topologię i konfigurację sieci lokalnej; parametry techniczne urządzeń, w tym centralnych urządzeń gromadzenia danych (serwery, macierze), zarządzanie uprawnieniami, bezpieczeństwo oprogramowania wykorzystywanego przez klienta; zasilanie awaryjne; system kopii zapasowych; ochronę przed kodem złośliwym i kodem mobilnym; monitoring sprzętu, systemów operacyjnych i oprogramowania; ciągłość działania; pracę zdalną; postępowanie z nośnikami danych; zarządzanie incydentami; umowy z dostawcami usług przechowywania danych. Dodatkowo u omawianego klienta dochodziło wykonanie testów penetracyjnych, przeprowadzenie badania ankietowego wśród pracowników oraz testy socjotechniczne.

Przedstawiony zakres prac został wyceniony przez firmę, która wygrała, na 3198 zł brutto. Czy na takim poziomie może zostać przeprowadzony audyt w tak szerokim zakresie za taką kwotę? Trudno byłoby nawet uwierzyć w takie wyceny tej usługi, gdyby nie publikacja wyników w BIP lub ich wysłanie do oferentów.

> *Zastanawiam się czasami, czy audytorzy zdają sobie sprawę z ciążącej na nich odpowiedzialności?*

Casus z lubelskiego

Przy okazji projektu Cyfrowa Gmina i Cyfrowy Powiat wiele urzędów zdecydowało się objąć działaniami audytowymi również jednostki podległe. Zgodnie z regulaminem grantu, diagnoza cyberbezpieczeństwa musiała zostać przeprowadzona tylko w urzędzie nawet w przypadku wydatkowania środków na jednostki podległe. W jednym z zapytań ofertowych (województwo lubelskie) należało wycenić wykonanie diagnozy cyberbezpieczeństwa dla Starostwa Powiatowego oraz 14 jednostek podległych. Wśród nich były: szkoły, DPS, Specjalny Ośrodek Szkolno-Wychowawczy, Środowiskowy Dom Samopomocy, Poradnia Psychologiczno-Pedagogiczna czy Powiatowy Urząd Pracy. W przypadku kilku jednostek mieliśmy do czynienia z podmiotami przetwarzającymi dużą ilość danych szczególnej kategorii, które generują potencjalnie największe ryzyko w przypadku zaistnienia incydentu czy naruszenia. Diagnoza miała zostać przeprowadzona w standardowym zakresie zgodnie z załącznikiem do projektu. Jednostki znajdują się od siebie oraz od starostwa w odległości od kilku do kilkunastu kilometrów. Wpłynęło osiem ofert z terenu całej Polski. Wygrała oferta firmy oddalonej o 500 km od siedziby zamawiającego. Usługa przeprowadzenia diagnoz we wszystkich wskazanych podmiotach (łącznie 15 podmiotów) została wyceniona na 15 240 zł, co na jednostkę daje 1000 zł brutto.

W zapytaniach ofertowych lub OPZ dopuszczane było zdalne przeprowadzenie audytu, co usprawiedliwiało podawanie tak niskich cen. Bardzo często zdalne wykonanie diagnozy polegało na wysłaniu ankiety do urzędu z prośbą o uzupełnienie tabeli, czyli klient tak naprawdę płacił za podpis audytora i jego certyfikat. Zastanówmy się, jaką wartość ma taki raport. Skoro osoby zajmujące się audytami na co dzień miały kłopoty z interpretacją i oceną poszczególnych obszarów, to jak dokonał tego IOD czy ASI w urzędzie? Jaka jest pewność, że audytowani przekazywali prawdziwe informacje?

Założenia projektów Cyfrowa Gmina oraz Cyfrowy Powiat są jak najbardziej słuszne, a obowiązek wykonania audytu określającego poziom bezpieczeństwa w JST jest jak najbardziej zasadny.

> *Zmienić należy natomiast sposób opracowywania wzoru diagnozy, jej metodologię, określanie kryteriów audytowych. Niezbędne jest również, aby oprócz certyfikatu audytor mógł się wykazać doświadczeniem popartym referencjami.*

Trudno powiedzieć, jak długo będziemy czekać na te niezbędne zmiany. Właśnie ruszył projekt Cyberbezpieczny Samorząd, stanowiący kolejny etap procesu podnoszenia poziomu cyberbezpieczeństwa w JST, i ponownie nie ma innych wymagań wobec audytora oprócz posiadania certyfikatu. Zapewne znów będziemy mieli do czynienia ze zjawiskiem „cena czyni cuda"…